CyberSecurity & Keeping your data safe

Medway Business Council
John Haddad, Bisinet Technologies
October 20, 2015

BISINET TECHNOLOGIES

We are under attack!!!

2013
110 million records compromised

2014
56 million payment cards compromised

2006-2007
46 million records compromised

2011
102 million records compromised

But this is Medway!
Who's going to attack my small business?

Jetpack

9,421
Blocked malicious login attempts

Capital Lender – mid-sized business (6 months)

Wordfence™

Top 5 IP's Blocked

IP	Country	Block Count
80.91.22.33	RU	488

Update Blocked IPs

Top 5 Countries Blocked

Country	Total IPs Blocked	Block Count
RU	2	488

Update Blocked Countries

Small Law Firm Site (1 week)

Wordfence™

Top 5 IP's Blocked

IP	Country	Block Count
37.115.190.97	UA	48
46.118.158.176	UA	29
173.192.104.148	US	6
159.224.139.133	UA	6
182.92.105.15	CN	5

Update Blocked IPs

Top 5 Countries Blocked

Country	Total IPs Blocked	Block Count
UA	14	85
US	37	51
ZA	15	19
IN	13	14
GB	10	13

Update Blocked Countries

Small Business Site (1 week)

Wordfence™

Top 5 IP's Blocked

IP	Country	Block Count
66.33.205.34	US	92
185.56.82.14	NL	40
100.42.63.193	US	10
92.43.19.165	ES	3
74.116.73.130	US	2

Update Blocked IPs

Top 5 Countries Blocked

Country	Total IPs Blocked	Block Count
US	4	105
NL	1	40
ES	1	3

Update Blocked Countries

Youth Sports Site (1 week)

So, what can businesses do to mitigate risk?

Things you can do starting tomorrow

1. Password Hardening
2. Personal Computers
3. Servers and Network Devices
4. Email & Encryption
5. Web Sites
6. Backup, Recovery & Business Continuity

Password Hardening
Most critical things you can do

- Change passwords every 90 days (minimum)
- **Strong** Passwords
  - Min 8 characters, 10-12 better
  - Mix UPPERcase, lowercase, numbers, symbols
  - Computer guess of passwords (www.howsecureismypassword.net)

Password	How long for a PC to guess it?
medway	0.07 seconds
Medway455	39 days
Medw@455$	58 years

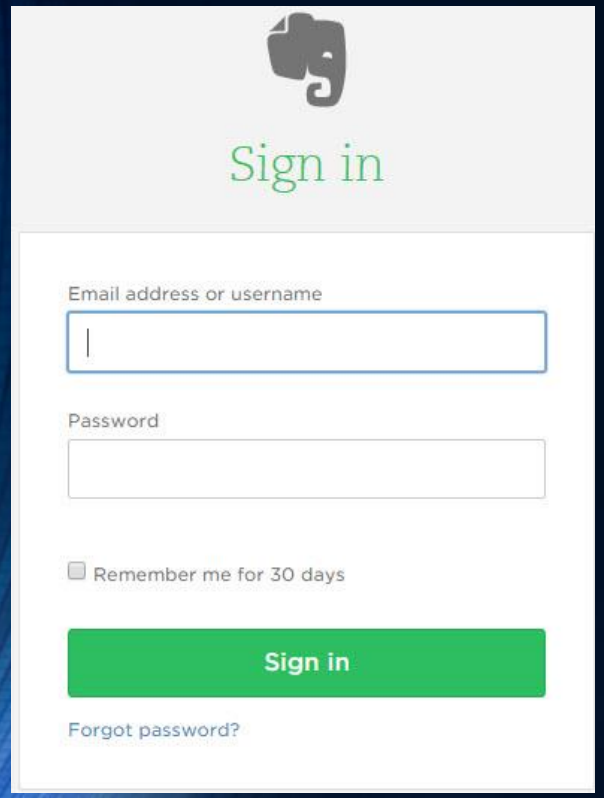
- Use Secure Password Managers (LastPass, Dashlane, 1Password, etc)

Password Hardening
Most critical things you can do

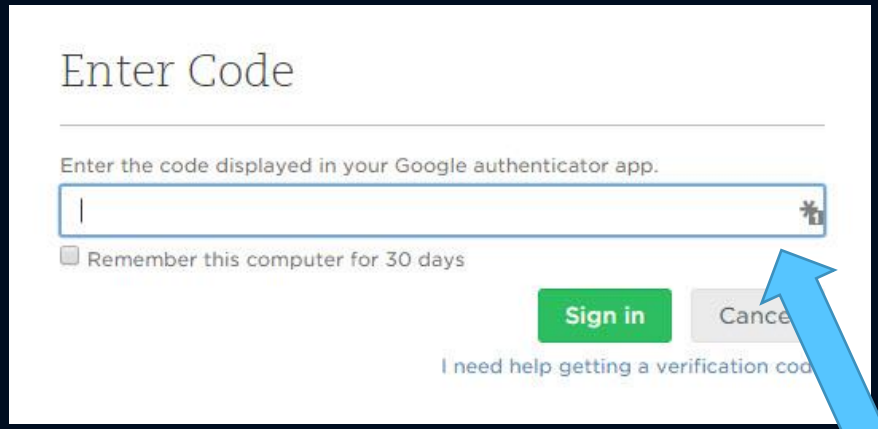
- Single Sign-on
  - One password gets you into several applications
  - Large companies deploying this, however, you can see this today with Google, Facebook and others
- 2-Factor Authentication
  - What you know (password)
  - What you have (token, smartphone, SMS)
- Many apps today support 2-factor authentication
  - Google/Gmail, Facebook, LastPass, Evernote, Dropbox, PayPal, Twitter, Salesforce.com, Microsoft Accounts (www.twofactorauth.org)
  - Use of smartphone – Google Authenicator app or SMS text

Password Hardening

How does 2-factor authentication work?



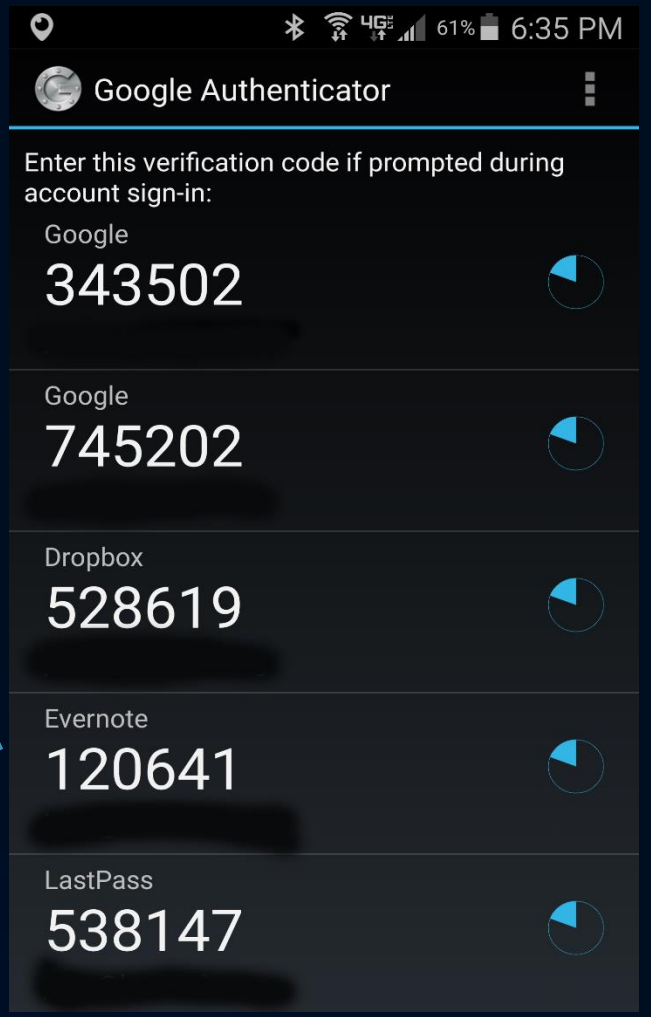
1. Enter username and password



2. Prompted to enter code displayed on your smartphone

3. Look for current generated code on smartphone (changes every minute)

4. Enter code into application and sign in



Personal Computers
Recommendations

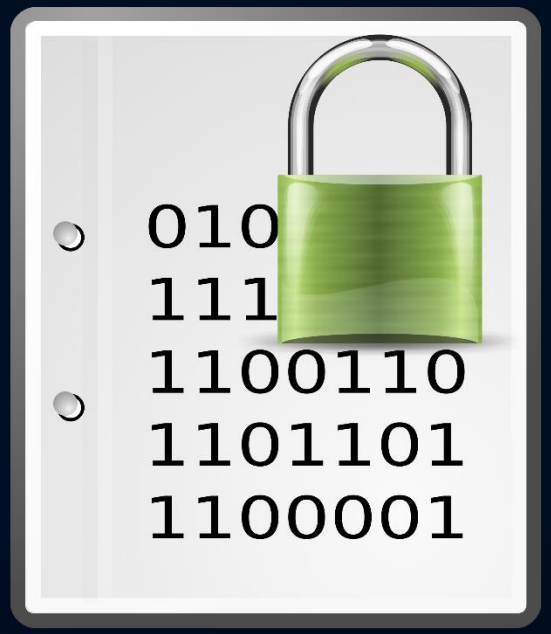
- Remove Admin capability from employee's PCs
  - Prevents from installing rouge software
  - Locks down what you want on the PC
- Force change of passwords every 90 days (min)
- Get employees into habit of locking PC when walking away
  - Auto-lock of PC after 15 minutes of non-use
- USB Sticks – Dangerous, especially when "free"!
  - If you must, use purchased, encrypted USB sticks
- Acceptable use policy
  - Make it clear in writing what is acceptable and non acceptable use of your company assets

Servers & Network Devices
Recommendations

- No "Admin" login on any devices
  - Many devices come with "admin" as default – change immediately
- Frequent change of passwords (min 90 days)
- Limit who has admin access
- Set up guest access for wireless networks
  - Control what can be accessed
- Physical Security
  - Lock devices in separate room – if possible – limit access
  - Proper ventilation / keep away from water!

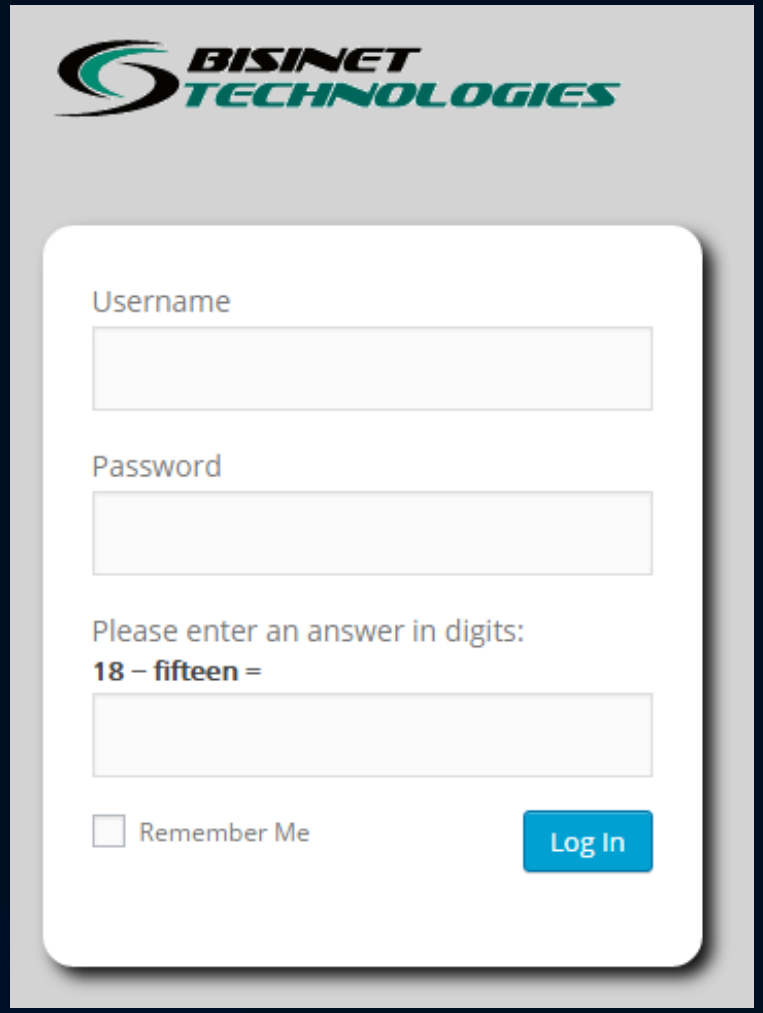
Email & Encryption
Recommendations

- Email filters and scanners in front-end email server
  - Filter spam & strip dangerous attachments
  - 50% of email hitting company servers is spam
- Encrypt emails – must for organizations transmitting sensitive information and documents
- Document clear email policies on use of company email by employees (e.g. non-personal use)
- Encrypt entire laptop hard drives
  - Especially for frequent travelers
  - Most PCs, Windows and Mac, come with encryption software built in



Web Sites
Recommendations

- No "Admin" logins
  - First thing every hacker tries on backend logins
- Force use of strong passwords for your employees & customers
- Enable latest CAPTCHA technology
- Limit login attempts
  - Brute force attacks will constantly hit your login
  - Lock out the IP address after "X" login attempts
- Firewall on web server to block unwanted traffic
  - e.g. - Block access outside US if only doing business domestically



Data Backup, Recovery & Business Continuity

Are you prepared for business disruption?

- BACKUP, BACKUP … then BACKUP
  - Both local backup and off-site backup (cloud)
  - Frequency depends on nature of business
  - Servers, Web Sites, PCs, Network configs
- Test Data Recovery
  - Backup is great, but do you know how to recover your data?
  - Have you tested data recovery each year?
- Questions to ask – Business Continuity
  - How long can your business afford to be "down"?
  - Do you have a plan and processes in place to recover in case of a disaster?

Thank You

John Haddad
Principal & Managing Director
Bisinet Technologies, LLC
john@bisinet.com

Web Site: www.bisinet.com
Blog: www.bisinet.com/our-blog